SPECIFICATION

TITLE

METHOD OF SECURE DATA TRANSMISSION

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] **The invention relates to a method of transmitting data securely in which redundant messages are transmitted.**

Description **of the Related Art**

[~~Method of secure data transmission~~]

[~~1. What technical problem is intended to be solved by your invention?~~]

[~~2. How has this problem been solved up until now?~~]

[~~3. In what way does your invention solve the specified technical problem?~~]

[~~4. Exemplary embodiment(s) of the invention.~~]

[0002]][~~1.~~]Many transmission media/protocols have [~~the~~]**a transmit-receive** property [~~that~~]**in which** messages transfered to [~~the~~]**a** medium by the transmitter arrive at the receiver in the same way (assuming that they arrive **at all**) [~~in which~~]**that** they were transmitted. In other words, message overhaul does not take place. Many protocols ensuring secure message transmission have this **transmit-receive** property as a prerequisite for the underlying transmission media/protocols which they use, since this **transmit-receive** property makes it much simpler to ensure efficient, secure message transmission. [~~The~~]**Historically, there has been a** problem[~~now is that~~] of defining protocols for secure message transmission which do not require this **transmit-receive** property **(i. e., possibly having message overhaul).**

[0003] ~~2.~~ **The following methods are** ~~used for this purpose or may be used for this purpose: although~~**(or may be) used for th purp s of defining such protoc ls. Alth ugh a prerequisite of th MTP standard (cf. Q.700 to Q.706)** ~~is~~**involves transmission media on which message overhaul cannot take plac ,**

MTP Level 2 (Q.703) is also able to operate with transmission media which do not have ~~this property.~~ the transmit-receive property.

[0004] [~~2.~~][~~The following methods are~~][~~used for this purpose or may be used for this purpose: although~~][~~a prerequisite of the MTP standard (cf. Q.700 to Q.706)~~][~~is~~][~~transmission media on which message overhaul cannot take place, MTP Level 2 (Q.703) is also able to operate with transmission media which do not have~~][~~this property.~~]It is fundamental to the operation of the protocol (Basic Error Correction), even in the case of message overhaul, that the MTP recognizes after a retransmission request whether a particular message has been sent on the basis of the retransmission request (it is then accepted), or whether it was actually sent before the retransmission request (it is then discarded). However, a disadvantage of this protocol is that it has no selective retransmission mode, which can be inefficient. In addition, without modification of MTP Level 2, the entire available bandwidth would be used, which may be disadvantageous.

[0005] MTP Level 2 with **the** Preventive Cyclic Retransmission method can also operate with message overhaul, since no retransmission requests are generated and messages which do not arrive in the correct order are discarded. [~~The~~]**Again, the** disadvantage of the method is [~~again~~]**a** poor utilization of the bandwidth.

[0006] TCP, which uses IP as underlying network protocol, has also solved the problem. Transmitted blocks which are not acknowledged are retransmitted when a timer has run out. [~~The~~]**This** protocol mechanism (**in which** only blocks received without gaps **are** acknowledged) results in unnecessary retransmissions, depending on the round trip delay[~~,~~] (even if the acknowledgement timeout is chosen to be long enough[~~,~~]) since the acknowledgement timer often also runs out for messages which have been received correctly after a lost message.

[0007] The situation is improved somewhat by methods such as Fast Retransmission and **providing an** explicit NACK upon the first occurrence of a gap.

[0008] The Reliable Data protocol works in a similar way to TCP, with the extension that messages which are not received without gaps can also be acknowledged.

SUMMARY OF THE INVENTION

[0009] [~~3.~~——]The present invention [~~discloses how~~] **xtends and modifies** certain existing protocols [~~can be extended/modified~~]in order to ensure efficient, secure data transmission using transmission media[~~/~~] **and** protocols in which message overhaul can take place.

[0010] In this context, the present invention is based on the realization that, for a modern protocol which is intended to work efficiently[~~,~~] (i.e., more rapidly[~~,~~]) using a transmission medium/protocol with possible message overhaul[~~-[lacuna]]~~, **and having** loss detection with minimization of unnecessarily transmitted information, the following properties are advantageous:

a) multiple selective retransmission method without full dependency on a timer; specifically, the loss of an ACK should not result in retransmission,

b) explicit status alignment between **a** transmitter and receiver,

c) retransmission of a message only if there is a certain probability that the message is lost,

d) messages received a plurality of times must not cause an incorrect response, **and**

e)[~~-it should be possible to-~~] use **of** parameter value selection to determine the tradeoff between rapid error correction and minimum unnecessary message transmission.

[0011] The most important of these points is point (d). Specifically, there are two opportunities/**situations** for messages received more than once to cause incorrect responses:

i) the message is recognized as having already been received, and this is defined as an error in accordance with the protocol**; and**

ii) the message is interpreted as a new message and triggers an action which later results in an error being detected in a transmitter or receiver as a consequence. By way of example, a supposed message loss may be detected by virtue of such a message. This results in a

retransmission request for messages which have not actually been sent yet, which is interpreted as an error by the transmitter.

[0012] One option for guaranteeing item (d) in protocols which satisfy the other items sufficiently, but not item (d), is for a message transmitted for the second time or more to be specially marked. Such protocols can then easily be changed so that such **marked** messages are simply ignored in the situations described under (i) and (ii).

[0013] Another opportunity to eliminate situation (i) is to ignore such messages as a general rule.

[0014] For **situation** (ii), a window [~~could~~]**can** also be defined[,] so that messages received outside of this window are generally ignored and do not result in any retransmission requests.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Exemplary embodiments of the invention are explained in more detail with the aid of figures.

Figure 1 is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 3 of the ITU-T Recommendation Q.2110;

Figure 2 is a data structure diagram showing the structure of the Poll Protocol Data Unit (SD-PDU) according to prior art Figure 4 of the ITU-T Recommendation Q.2110;

Figure 3 is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 5 of the ITU-T Recommendation Q.2110;

Figures 4A & 4B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of th present invention;

Figures 5A & 5B are flowchart segments showing the SSCOP pr cessing according to Figur 20, sheet 43 of 51, of the

ITU-T Recomm ndation Q.2110 as modified by method 1 of the present invention;

Figures 6A & 6B ar flowchart segments showing the SSCOP proc ssing according to Figure 20, sheet 44 of 51, of th ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;

Figures 7A & 7B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of th ITU-T Recommendation Q.2110 as modified by method 2 of the present invention; and

Figure 8 is a flowchart segments showing the SSCOP processing according to common elements of Figure 20, from sheets 40, 41, 43 and 44 of 51, of the ITU-T Recommendation Q.2110.

DETAILED DESCRIPTION OF THE INVENTION

[0016] [4.——]The exemplary embodiment chosen is the protocol **Service Specific Connection-Oriented Protocol** (SSCOP) described in **ITU-T Recommendation** Q.[2110.]**2110 (07/94) - B-ISDN ATM ADAPTATION LAYER - SERVICE SPECIFIC CONNECTION ORIENTED PROTOCOL (SSCOP) Q.2110 (herein incorporated by reference).** This protocol fulfills the properties [3][(a[[, 3b and 3]) **through (c) identified above**, but has the problems described under [3][(i) and [3][(ii). Specifically, [3]**when the message is recognized as having already been received and this is defined as an error in accordance with the protocol (i), this** results in an incorrect response (branch to the connector D) in **ITU-T Rec.** Q.[2110, figure 20]**2110** ([sheet 40 of 51]**Figure 4B**). Similarly, [figure 20 (sheet 40 of 51) in Q.2110 shows]**Figures 4A and 4B show** that a message having the property [presupposed]**described** in [3][(ii) usually results in a retransmission request (USTAT). This in turn usually results in a branch to the error branch (connector D) in [figure 20 (sheet 43 of 51)]**Figur 5B**.

[0017] In one embodiment of the invention, **method 1,** in accordance with [3)]**the discussion above**, [an]**a Sequenced Data Protocol Data Unit** (SD-PDU)

is now specially marked in the case of repeated transmission, e.g., by setting bit 5 in the PDU trailer ([~~cf. figure 3/Q.2110~~]**Figure 1, th RX field**) to [~~1.~~]**1 (Figure 5A, 5.1), indicating a repeat d transmission. This embodiment modifies the ITU-T Rec. Q.2110,** Figure 20 (sheet 40 of 51)[~~in Q.2110 is modified~~] such that, in the two error situations described above, a check is first carried out to determine whether the SD-PDU is marked as having been repeated **(Figure 4A, 4.1)**. In this case, the message is ignored and an incorrect response cannot occur.

[0018] [~~Alternatively,~~][~~figure 20 (sheet 40 of 51)~~][~~in Q.2110~~][~~is modified such that the error case~~][3][~~i) is generally not checked, and a message which has already been received is simply ignored~~][~~.~~][~~In addition, likewise in~~][~~figure 20 (sheet 40 of 51)~~][~~,~~]

]**Alternatively, in method 2, the ITU-T Rec. Q.2110** ~~Alternatively,~~ **figure 20 (sheet 40 of 51)** ~~in Q.2110~~ **is modified such that the error case** ~~3~~**(i) is generally not checked, and a message which has already been received is simply ignored.** ~~-~~ **(Figure 7B, 7.2, TRUE path). In addition, likewise in Figure 7A, the ITU-T Rec. Q.2110 figure 20 (sheet 40 of 51),** ~~-~~ **is modified such that,** after the query VR(H) < VR(MR), a check is carried out to determine whether SD.N(S) < VR(R) + [~~2**23,~~]**2^{23}**, for example **(Figure 7B, 7.2)**. (This presupposes that the window size used for the flow control is always smaller than [~~2**23,~~]**2^{23}**, which does not represent any relevant restriction, however). If this is not the case, the message is discarded **(Figure 7A, 7.1, FALSE path)**, otherwise it is handled as previously.

[0019] Item (e) can also easily be achieved with SSCOP, e.g., USTATs could be sent only with a certain time delay, in order to wait for messages which have been repeated. In addition, it would be possible for only gaps which have already existed for a certain time to be reported (or heeded) using/in the case of a STAT.

[0020] **The above-described methods are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scop of the present invention.**